**IP-240-03, Rev. 2**

**Date 1/20/09**

**Environmental Management Consolidated Business Center (EMCBC)**

**Subject: Software Application Development and Management**

Implementing Procedure APPROVED: *(Signature on File)*

ISSUED BY: OFFICE OF INFORMATION RESOURCES MANAGEMENT

## 1.0 PURPOSE

The purpose of this procedure is to define the process for Software Application Development and Management.

## 2.0 SCOPE

This procedure is for all applications developed by the Office of Information Management (IRM) that utilize data management software such as MYSQL, ORACLE, SQL Server, etc.

## 3.0 APPLICABILITY

This procedure is applicable to all general application development activities. It is not applicable for Applications requiring the development of an Exhibit 300 (financial applications over $500k per year, other applications costing over $5,000k over three years, or designated “Critical Systems”) or to Nuclear Safety Software.

## 4.0 REQUIREMENTS and REFERENCES

4.1 Requirements:

4.1.1 System Security Plan for General Support System, PL-240-08

Section:

4.1.1.1 SI-2 Flaw Remediation
4.1.1.2 SI-3 Malicious Code Protection
4.1.1.3 SI-10 Information Input Accuracy, Completeness and Validity
4.1.1.4 SI-11 Error Handling
4.1.1.5 SI-12 Information Output Handling and Retention
4.1.1.6 SA-11 Developer Security Testing

4.1.2 EMCBC Policy PS-240-06, on the Control of Unclassified Electronic Information

4.2 References:

4.2.1 Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) -Application Security Checklist

http://iase.disa.mil/stigs/stig/application_security_and_development_stig_v2r1_final_20080724.pdf.

4.2.2 (FIPS) Publication 127-2 Federal Information Processing Standards Database Language SQL, 1993 June 02

4.2.3 EMCBC Implementing Procedure (IP)-240-05, Control and Development of Technical Instructions and Documents

4.2.4 EMCBC IP-240-02, Configuration Management of Computer Systems and Networks.

4.2.5 DOE N 203.1, Software Quality Assurance

4.2.6 DOE O 414.1C, Quality Assurance

4.2.7 EMCBC PS-243-01, Records Management Policy,

4.2.8 DoD 5015.2-STD Electronic Records Management Software Application Design Criteria standard, 2007

4.2.9 Records Policy, Guide to IT Capital Planning and Investment Control (CPIC), September 2005

## 5.0 DEFINITIONS

5.1 System Owner: The lead IRM individual that has overall implementation responsibility for any given Application. Usually the Assistant Director for Information Resource Management

5.2 Content Owner: The Assistant Director responsible for the content within the given application or system

5.3 Content Manager: Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.

5.4 Developer: IRM staff responsible for coding, testing, and placing the application into production.

5.5 Alpha Testing: Testing of applications with inert data (made up data).

5.6 Beta Testing: Testing of applications with “real” data.

## 6.0 RESPONSIBILITIES

6.1 System Owner will

6.1.1 Approve the completed Project Plan.

6.1.2 Establish the Data Base Management System and applicable user interface.

6.1.3 Provide the test and baseline actions required to certify or recertify the application for production.

6.1.4 Conduct a Make or Buy analysis & oversee the procurement.

6.1.5 Include elements of Software Quality Assurance applicable to specific projects.

6.1.6 Conduct annual Application review.

6.1.7 Approve requests for software changes

6.2 Content Owner will

6.2.1 Approve the completed Project Plan.

6.2.2 Complete Software Quality Assurance Checklist

6.3 Developer shall

6.3.1 Assist in development of the Application Project Plan

6.3.2 Develop the code for the application

6.3.3 Assure that the application is brought into Configuration Management

6.3.4 Resolve punch list items

6.3.5 Conduct testing and develop Baseline Change as necessary.

6.4 Content Manager shall

6.4.1 Develop Application Project Plan

6.4.2 Develop an analysis of the life cycle requirement for the application.

6.4.3 Develop a proposed schedule for completion.

6.4.4 Develop a punch list for changes or correction during testing phases.

6.4.5 Develop changes and revisions to Application Project Plan during the life cycle.

6.5 Independent Reviewer shall

6.5.1 Conduct Software Quality Assurance review when such a review is required. The individual assigned as the Independent Reviewer shall not also act in any of the following roles: System Owner, Content Owner, Content Manager, and Developer for the application in question.

## 7.0 GENERAL INFORMATION

This procedure provides for a structured process for the inception, design, development, and testing of applications developed by the EMCBC. The intent of this procedure is to provide for a fluid and streamlined inception and design phase followed by a rigorous test phase to ensure that all data meets the requirements for availability, integrity, and security.

Software development is a complex, iterative process in which Software Quality Assurance (SQA) principles play an important role. This procedure does not provide a detailed implementation for all tasks associated with developing or maintaining DOE software. Rather it provides the framework for controlling, managing and documenting that process. The System Owner is responsible for including those elements of SQA applicable to the specific project.

8.0 PROCEDURE - Applications can cover a wide variety of data control and manipulation. They range from a simple application with a single table to support simple queries on a webpage to complicated multi tabled databases containing sensitive data with intricate user interface. Application Development and Management is controlled through a seven phase process, Initiation, Application Definition, Development, Baseline Testing, Production, Revision and Maintenance, and Retirement.

8.1 Initiation Phase – The initiation process is started when a perceived need for an application to accomplish a specific task or group of task is developed. This need is presented to the IRM staff and from there informal discussions formulate the concept and general scope of the proposed application. Once a concept has been formulated the Assistant Director of Information Resource Management (ADIRM ) will determine if the proposed application is viable and if resources are available to pursue the development. Discussion at the management level will determine if the development will go forward and to align the project schedule with the priorities of the organization.

8.2 Application Definition – Once there is a general agreement among management to proceed the requesting organization will establish an Application Project Plan. Application Project Plans are controlled as Technical Instructions Documents (TIDs) in accordance with IP-240-05, Control and Development of Technical Instructions and Documents (Reference 4.2.3). This project plan will define the overall objectives of the application, define the key roles of System Owner, Content Owner, Content Manager, Developer and provide the following information:

8.2.1 Statement of Need – The Content Manager shall create a Statement of Need that will define what need is being fulfilled by the application. It should also address the functionality of the system, who needs to access the system, how often, and where are they located. Also this section should discuss reporting requirements and any manipulation of data required. The generation of a flow chart that shows the flow of data is encouraged and may be required by the Developer to assist in application design.

8.2.2 Data Set – The data set is the entirety of the type of data that the application will be manipulating.

8.2.2.1 Data type - The Data type should be described by description or title, approximate length, and if it is a member of a subset of data.

8.2.2.2 Data Sensitivity – The Data Set shall also identify the sensitivity of the data in accordance with the EMCBC Policy on the Control of Unclassified Electronic Information. Attachment (A) has a summary chart from the policy.

8.2.2.3 Software Quality Assurance Checklist – Utilizing Attachment (B), the proposed purpose and functionality of the software is assessed to determine the need for a Software Quality Assurance Review.

8.2.2.4 Records Management –Utilizing Attachments (C) and (D) as guidance, the Records Management Implications of the proposed application is determined.

8.2.3 Security Requirements – Once the Data Sensitivity has been established the security and access requirement will be developed by the Developer and documented in the Project Plan. At a minimum all applications are tested for SANS (SysAdmin, Audit, Network, and Security Institute) Top 20 Vulnerabilities (http://www.sans.org/top20/).

8.2.4 Development Schedule – The Content Manager will develop a proposed schedule for completion.

8.2.5 Life Cycle Analysis – The Content Manager will develop an analysis of the life cycle requirement for the application and shall indicate a time frame for Application Retirement and final disposition.

8.2.6 Once all of the above data elements are contained in the Project Plan the System Owner will conduct a Make or Buy analysis. This analysis should include Commercial off the shelf (COTS), Government off the shelf (GOTS), and the compatibility of other in-house applications or applications from other sites and reflect the criteria for SQL databases contained in the Federal Information Processing Standards (FIPS) 127-2.

8.2.6.1 Once the analysis is complete the System Owner will determine how the application will be implemented. If purchased, the System Owner will oversee the procurement, and if by in-house development the System Owner will establish the Data Base Management System and applicable user interface.

8.2.6.2 Applications with a rough cost estimate of fewer than 80 hours of internal resources do not require documented make or buy decision.

8.2.7 Approval – The Content Manger and the System Owner will approve the completed Project Plan.

8.3 Development Phase – The assigned Developer shall proceed with developing, modification, or installation of the application. The Developer will work closely with the Content Manager to ensure that all the requirements of the Project Plan are being implemented.

8.3.1 Changes – During the course of all development there is a need for changes that where not anticipated during the Project Plan development. For the most part changes are minor and do not affect the development requirements established in the Project Plan. However, if there are any changes made that would affect the sensitivity of the data or the types and locations of users accessing the data, the Project Plan will be updated to reflect the new needs and the Data Sensitivity and Security Requirements will be reexamined.

8.4 Baseline and Acceptance Testing – This phase has three distinct sub-phases, Alpha Testing, Baselining, and Beta testing. A Software Quality Assurance Review, when such a review is determined to be required by the Software Quality Assurance Checklist, Attachment B, is conducted as appropriate by the Independent Reviewer during this period. The complexity of the Software Quality Assurance Review may be as simple as an independent review of the output or as complex as a detailed Software Quality Assurance Test Plan.

8.4.1 Alpha Testing is conducted once the Developer releases the application to the Content Manager for initial testing. This may be done in whole or in part at the discretion of the Developer and the Content Manager. Alpha testing may be done in-house or from remote locations. However, **ALL ALPHA TESTING IS CONDUCTED WITH INERT DATA.** Real data is not to be used during alpha testing as it could very easily expose sensitive data. At the end of alpha testing the Content Manager will develop a punch list for changes or correction. Any major changes to the application will require a revision to the Application Project Plan.

8.4.2 Baselining is conducted in accordance with IP-240-02, Configuration Management of Computer Systems and Networks, (Reference 4.2.4). This process ensures that all cyber security controls are in place and functioning. Security Testing will be conducted in accordance with the applicable Technical Instructions. Application specific security tests will be developed as needed and updated in the appropriate Technical Instruction.

8.4.3 Beta Testing, testing with live data, begins once the Application baseline has been established. At the end of Beta testing the Content Manager will again develop a punch list of items that need correction.

8.5 Production – Once all testing and security items have been resolved and with the concurrence of the Content Owner and System Owner the application is considered to be certified and is placed into production.

8.6 Revision :

8.6.1 Minor Changes may be made in accordance with the provision of IP- 240-02

8.6.2 If a major revision (such as a change in data sensitivity, application access process, results of the Software Quality Assurance Checklist or as deemed necessary by the System Owner) to the application is required, the Content Manager will develop an addendum to the existing Application Project Plan to clearly define the needed changes. The System Owner will provide the necessary test and baseline actions, including a Software Quality Assurance Review by an Independent Reviewer as appropriate, required to recertify the application for production.

8.6.3 All changes, minor & major, require the completion of the software change request form IP-240-03-F1 (Attachment E).

8.7 Annual Review – Each application will be reviewed annually by the System Owner to ensure that it is still needed and meets current security requirements. This review may be done in concert with other related applications. All reviews are documented in the IM Maintenance Log.

8.8 Retirement – At the end of the life cycle the application will be retired in accordance with the Application Project Plan.

## 9.0 RECORDS MAINTENANCE

Records generated as a result of implementing this document are identified as follows:

9.1 Application Project Plans – IRM record

9.2 Security Test Results – Application Log

9.3 Software Change Request Form, IP-240-03-F1

## 10.0 FORMS USED

10.1 Software Change Request, IP-240-03-F1

## 11.0 ATTACHMENTS

11.1 Attachment A - Summary Chart on Controls for Electronic Information

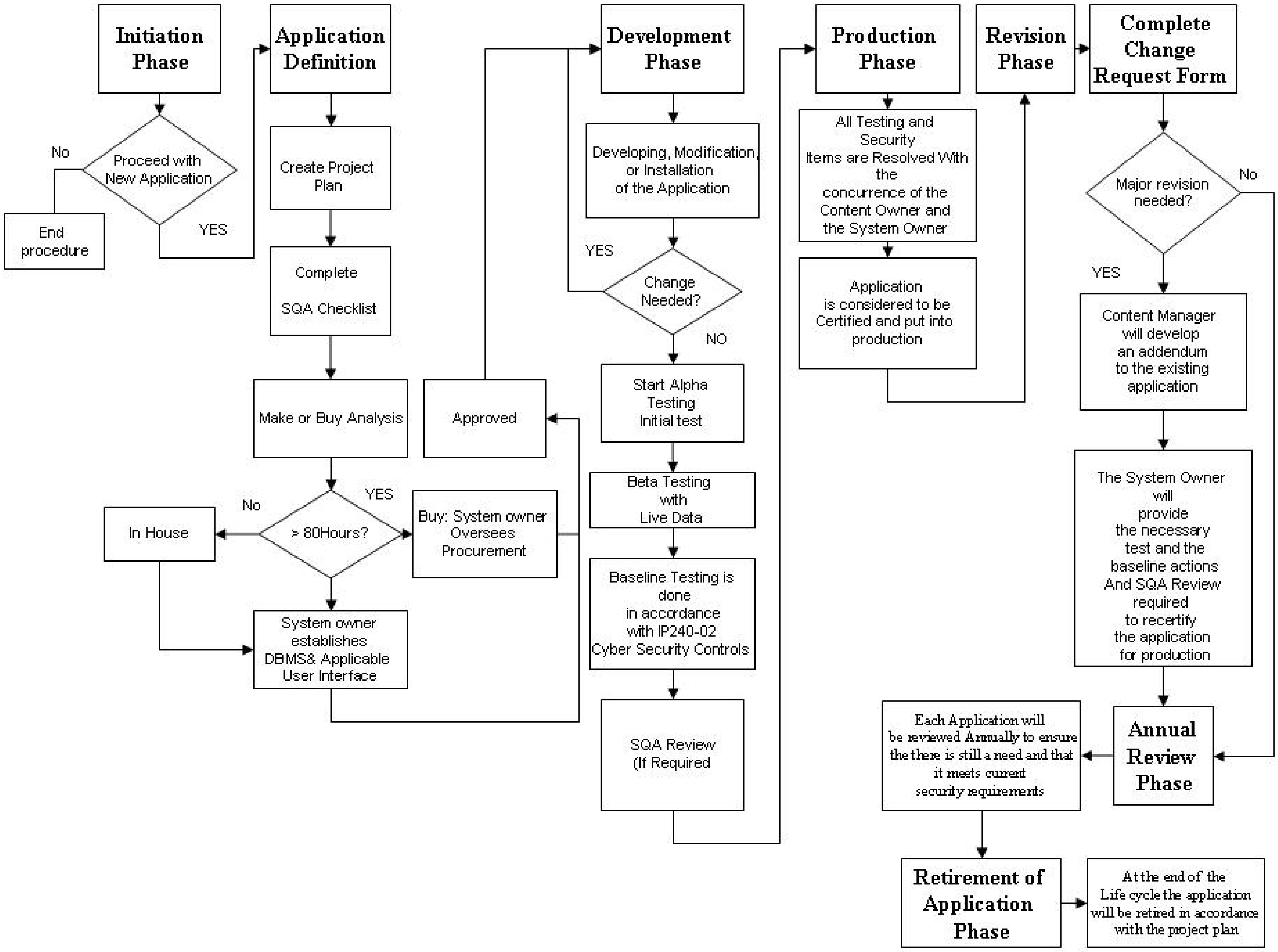
11.2 Attachment B – Software Quality Assurance Checklist

11.3 Attachment C - Records Management Compliance Checklist

11.4 Attachment D – Is It A Record?

11.5 Attachment E- Software Change Request , IP-240-03-F1

## 12.0 FLOWCHART


Initiation Phase
Proceed with New Application
No
End procedure
YES
Application Definition
Create Project Plan
Complete SQA Checklist
Make or Buy Analysis
> 80Hours?
No
YES
In House
Buy: System owner Oversees Procurement
System owner establishes DBMS& Applicable User Interface
Approved
Development Phase
Developing, Modification, or Installation of the Application
YES
Change Needed?
NO
Start Alpha Testing Initial test
Beta Testing with Live Data
Baseline Testing is done in accordance with IP240-02 Cyber Security Controls
SQA Review (If Required
Production Phase
All Testing and Security Items are Resolved With the concurrence of the Content Owner and the System Owner
Application is considered to be Certified and put into production
Revision Phase
Complete Change Request Form
Major revision needed?
No
YES
Content Manager will develop an addendum to the existing application
The System Owner will provide the necessary test and the baseline actions And SQA Review required to recertify the application for production
Annual Review Phase
Each Application will be reviewed Annually to ensure the there is still a need and that it meets current security requirements
Retirement of Application Phase
At the end of the Life cycle the application will be retired in accordance with the project plan

## Attachment A
## Summary Chart on Controls for Electronic Information

| Type | Definition | Control |
|---|---|---|
| I-PII | Data defined as PII by regulation or requirement | Data is only stored on network storage devices. Access is controlled by network credentials. Special authorization required for transportation on mobile devices. Users receive special training to ensure protection of this data. |
| I | Data that has been specifically defined as needing encryption by requirement such as Sensitive Unclassified Information | Data is stored or transported encrypted as required and, requires two factor authentication for remote access. Users receive special training to ensure protection of this data. |
| II | Business Sensitive Data – data that has a direct bearing on business decisions that if compromised could result in an unfair advantage to parties conducting business or in legal action with the department. Type II data is designated by the Content Owner | Data access is controlled through the network and requires two factor- authentications for remote access. Data is protected by encryption in transport. |
| III | Information about Business Sensitive Data that requires protection to ensure data integrity, and a level of confidentiality, or data needs to be screened from the general public. Type III data is designated by the Content Owner | Data access is controlled through the network, requires username and password for remote access. Files transported on removable media should be protected by password. |
| IV | Public data that may be released at anytime. Web site data makes up the bulk of this data | Data access is controlled through the network. Data is posted to the web as directed by the Content Manager. Precautions are taken to ensure data integrity. |

## Attachment B

# Software Quality Assurance Checklist

**Software Title(s)**______________________________________________

**Software Content Owner**__________________________________________

| YES | NO | * EVALUATION CRITERIA |
|---|---|---|
| | | **Management Requirement**<br>Does Management require a Quality Assurance review of this application based on factors other than listed below? |
| | | **Customer Interface**<br>Will this application be used by or will the output be viewed by our customers (public, DOE HQ, the SLA Sites, etc.)? |
| | | **Multiple Interfaces**<br>Will this application be used by multiple groups requiring multiple interfaces within the EMCBC organization? |
| | | **Sensitive Information**<br>Will this application process, store, or display sensitive information? |
| | | **Quality Assurance Implementation Plan**<br>Will this application impact one of the 10 criteria in the Quality Assurance Implementation Plan (Example: Personnel Training and Qualification, Issues Management, Records Management**, Procurement, etc.) |

* The Content Owner shall evaluate the need for a software quality assurance review. A software quality assurance review is required if any of the above requirements are met. The complexity of the software quality assurance review may be as simple as an independent review of the output or as complex as a detailed Software Quality Assurance Test Plan.

**Utilize RECORDS MANAGEMENT COMPLIANCE CHECKLIST, Attachment C, to determine the records implications for the proposed application

# Attachment C
# Records Management Compliance Checklist
# Adapted from the Recommended Management Process for CPIC (Capital Planning and Investment Control) Proposals

Section 1. Determination of Records Implications
A Yes answer to any questions below indicates that the proposed application has records implications. Include this determination in the Application Project Plan.

1. Does the proposed application replace a paper-based system that currently generates records?

2. Is the proposed application an upgrade or extension of an existing system that has been determined to have records implications?

3. Does the proposed application create or manage any of the following types of information? Unclassified? Official Use Only? Privacy Act? Quality Assurance? Vital Records? Permanent Records?

4. Based on the above information and Attachment D, (Is It a Record?), will the proposed application contain or produce or declare information to be records?

5. Is the proposed application an Electronic Records Management System (ERMS) that identifies records and applies retention periods?

Section 2. If the proposed application has records implications as per Section 1, include the following information in the Application Project Plan.

6. If the proposed application contains records (Yes to question 4) and is not an ERMS (No to question 5), does the functionality include the transfer of the records to a separate ERMS that meets DOE-STD-4001-2000?

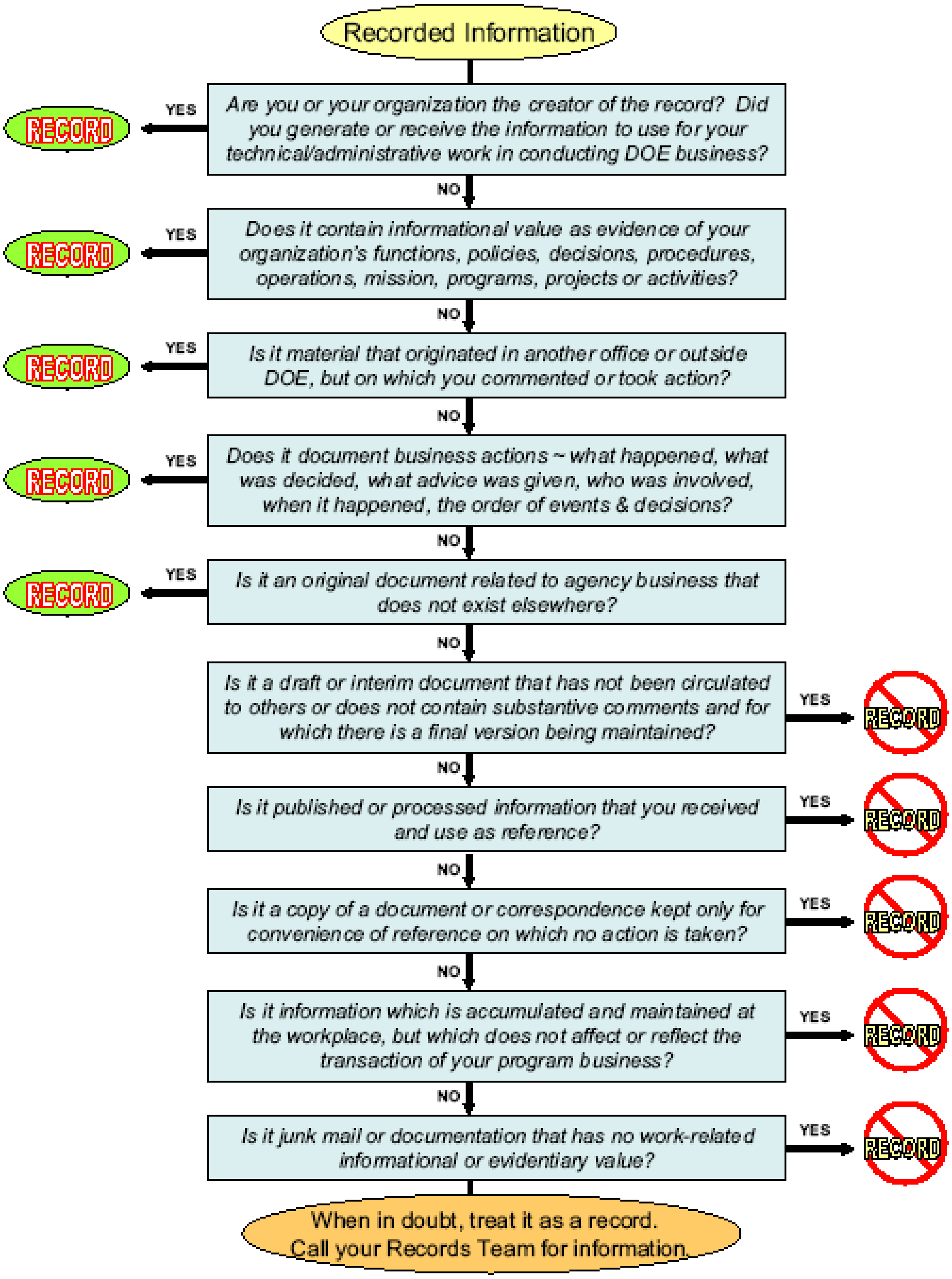
7. If the application is an ERMS (Yes to question 5), does the proposed application meet DOE-STD-4001-2000, “Design Criteria for Electronic Records Management Software Applications”?

8. If the proposed application contains records (Yes to question 4), is not an ERMS (No to question 5), and does not include functionality to transfer the records to an ERMS (No to question 6) then does the work process include printing the records in hardcopy ?

9. Describe how the software and metadata to support retrieval will be retained for the life of the information/record?

## Attachment D

## Is it a Record?



Recorded Information

Are you or your organization the creator of the record? Did you generate or receive the information to use for your technical/administrative work in conducting DOE business?

Does it contain informational value as evidence of your organization's functions, policies, decisions, procedures, operations, mission, programs, projects or activities?

Is it material that originated in another office or outside DOE, but on which you commented or took action?

Does it document business actions ~ what happened, what was decided, what advice was given, who was involved, when it happened, the order of events & decisions?

Is it an original document related to agency business that does not exist elsewhere?

Is it a draft or interim document that has not been circulated to others or does not contain substantive comments and for which there is a final version being maintained?

Is it published or processed information that you received and use as reference?

Is it a copy of a document or correspondence kept only for convenience of reference on which no action is taken?

Is it information which is accumulated and maintained at the workplace, but which does not affect or reflect the transaction of your program business?

Is it junk mail or documentation that has no work-related informational or evidentiary value?

When in doubt, treat it as a record.
Call your Records Team for information.

## Attachment E

**Software Change Request Form** **Form No**

| | | | | |
|---|---|---|---|---|
| **Requestor Name** | | | **Date Submitted** | |
| **Requestor Email** | | | **Requestor Phone** | |
| **Requestor Organization** | | | **Requestor Location** | |

| | |
|---|---|
| **Application Name** | |
| **Short description of request**<br>**(Attach detailed specification)** | |
| **Justification for change** | |
| **Classification of Data as per IP-240-03** | |
| **Will this change alter the results of the Software Quality Assurance Checklist of the application? If yes, explain.** | |
| **Target date** | |

### Review & Approval Status

| **Content Manager Approval** | | |
|---|---|---|
| **Name:** | **Signature:** | **Date:** |

| **IRM Approval** | | |
|---|---|---|
| **Name:** | **Signature:** | **Date:** |

## EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

l Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.

l Placing the words GENERAL REVISION at the beginning of the test.

| Rev. No. | Description of Changes | Revision on Pages | Date |
|---|---|---|---|
| 1 | Original Procedure | Entire Document | 1/22/07 |
| 2 | Added language to Heading | 1 | 1/20/09 |
| 2 | Added word “Software” in 1.0 | 1 | 1/20/09 |
| 2 | Added “SQL Server” to 2.0 | 1 | 1/20/09 |
| 2 | Added exclusion for Nuclear Safety Software to 3.0 | 1 | 1/20/09 |
| 2 | Added reference to PL-240-08 | 1 | 1/20/09 |
| 2 | Added link to 4.2.1 | 2 | 1/20/09 |
| 2 | Added references 4.2.5 – 4.2.9 | 2 | 1/20/09 |
| 2 | Added will and shall language in 6.1 – 6.5 | 3,4 | 1/20/09 |
| 2 | Added responsibilities 6.1.5, 6.1.7, 6.2.2 to existing roles | 3 | 1/20/09 |
| 2 | Added Independent Reviewer responsibility , section 6.5 | 4 | 1/20/09 |
| 2 | Added paragraph to 7.0 beginning with “Software development is a complex” | 4 | 1/20/09 |
| 2 | Defined ADIRM and added the phrase “to align the project schedule…” to 8.1 | 4 | 1/20/09 |
| 2 | Defined TID’s in 8.2 | 5 | 1/20/09 |
| 2 | Added clarification that the Content Manager creates the Statement of Need in 8.2.1 | 5 | 1/20/09 |
| 2 | Expanded 8.2 into 8.2.2.1 – 8.2.2.4 to clarify and to now include requirement for SQA checklist and Records Management issues | 5 | 1/20/09 |
| 2 | Defined COTS and GOTS in 8.2.6 | 6 | 1/20/09 |
| 2 | Changed “developer will” to “Developer shall” in 8.3 | 6 | 1/20/09 |
| 2 | Added language about SQA starting | 6 | 1/20/09 |

| | | | |
|---|---|---|---|
| | with “A Software Quality Assurance Review, when such a review is determined to be required…” to 8.4 | | |
| 2 | Corrected spelling “baselining” | 7 | 1/20/09 |
| 2 | Expanded section 8.6 to 8.6.1 – 8.6.3 to include requirement for SQA and new form IP-240-03-F1 | 7 | 1/20/09 |
| 2 | Added Software Change Request Form, IP-240-03-F1 to sections 9.0 and 10.0 | 8 | 1/20/09 |
| 2 | Added listing of Attachments B –E in section 11.0 | 8 | 1/20/09 |
| 2 | Added flowchart , section 12.0 | 9 | 1/20/09 |
| 2 | Added Type I-PII to Attachment Attachment 10 | 10 | 1/20/09 |
| 2 | Added Software Quality Assurance Checklist, Attachment B | 11 | 1/20/09 |
| 2 | Added Records Management Compliance Checklist, Attachment C | 12 | 1/20/09 |
| 2 | Added “Is It a Record” Attachment D | 13 | 1/20/09 |
| 2 | Added Software Change Request Form, Attachment E | 14 | 1/20/09 |

CONTROLLED DOCUMENT CHANGE REQUEST

DATE: _____9/24/2008___________________________

INITIATOR: _____W. Best ____________________________

INITIATOR PHONE NUMBER: _60530________________________________________

DOCUMENT AFFECTED: ___Application Development and Management__________

SECTION: _____ PARAGRAPH #:______

CONTROLLED NUMBER : IP-240-03___________ PARAGRAPH #:_______

NEW CONTROLLED NUMBER: IP-240-03,Rev.2

PROPOSED
REVISION: ______Add a form for software change requests, Add language for Records Management, add
Flowchart.____________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________

JUSTIFICATION: A more formal process for requesting software changes is needed to ensure changes are properly authorized. It is important to ensure that software applications that create or manage electronic records comply with Records Management policies and procedures.
________________________________________________________________________________
_____________________________________________

Requested by:
___W. Best __________________________ Date_9/23/08____________________

Approval:
______________________________ DATE: ______________________
Associate Director

Assigned to: _______________________ DUE DATE: _____________________

## Document Review Record Sheet

| | |
|---|---|
| Document Title | Application Development and Management |
| | |

| | | |
|---|---|---|
| Control Number | Revision No.<br>2 | Date Issued for Review<br>06/25/2008 |

The subject document is being submitted for your review, approval or comments. Since this review is controlled, a response is required from all reviewers. Therefore, please return the review sheet with or without comments

| | | |
|---|---|---|
| To:<br>L. Chafin | Extension:<br>60461 | By:<br>06/16/2008 |

Additional Instructions:

| Reviewer | Approve | Approve w/Comments | Do Not Approve | Signature of Reviewer |
|---|---|---|---|---|
| B. Fain | | | | |
| M. Roy | | | | |
| W. Best | | | | |
| L. Schlag | | | | |
| H. Taylor | | | | |
| R. Holland | | | | |
| T. Brennan | | | | |
| R. Everson | | | | |
| T. J. Jackson | | | | |
| J. Craig | | | | |

Comments may be attached to a separate sheet of paper

**APPROVE:** Signifies the reviewer's acceptance of the document issued for review.

**APPROVE w/comments**: Signifies the reviewer's overall acceptance of the document regarding concept, practice, implementation, provisions and assigned responsibilities. However, the reviewer has suggestions as to the organization of its contents or helpful additions and/or deletions. These comments are termed "non-mandatory comments" and do not require formal resolution between the reviewer and preparer.

**DO NOT APPROVE**: Signifies that the reviewer has identified significant problems regarding concept, practice, implementation or responsibilities that render the document unacceptable and/or not in conformance with stated requirements. Such problem areas must be clearly identified by the reviewer. It is mandatory for the preparer to resolve these comments with the reviewer document the resolution and obtain the reviewers concurrence for the resolution. The reviewer's written concurrence with the resultant change in disposition shall be documented on this form.

General Review Comments:

When review is delegated, the designated reviewer shall review and indicate concurrence with the designee's review comments and recommend disposition:

| Designated Reviewer | Concur | Do Not Concur | Signature | Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |